UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/759,596	01/15/2004	Christopher Newell Toomey	AOL0133	8695

22862 7590 05/31/2007

GLENN PATENT GROUP
3475 EDISON WAY, SUITE L
MENLO PARK, CA 94025

EXAMINER	
KHOSHNOODI, NADIA	
ART UNIT	**PAPER NUMBER**
2137	

MAIL DATE	DELIVERY MODE
05/31/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/759,596	TOOMEY, CHRISTOPHER NEWELL	
	Examiner	Art Unit	
	Nadia Khoshnoodi	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 March 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-5,8-10,12-38,40-42,45-47 and 49-94* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-5,8-10,12-38,40-42,45-47 and 49-94* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 January 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *2/3-06-2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

Claims 2, 6-7, 11, 39, 43-44, & 48 have been cancelled. Applicant's arguments/amendments with respect to amended claims 1, 8, 12-13, 17, 27, 29-30, 32-33, 38, 45, 49, 53, 55, 66-67, 69-70, 74, 78-82, & 90 and previously presented claims 3-5, 9-10, 14-16, 18-26, 28, 31, 34-37, 40-42, 46-47, 50-52, 54, 56-65, 68, 71-73, 75-77, 83-89, & 91-94 filed 3/6/2007 have been fully considered but they are not persuasive. The Examiner would like to point out that this action is made final (See MPEP 706.07a).

Information Disclosure Statement

In order for documents to be considered Applicants must file the IDS and furnish appropriate references (i.e. any cited NPL and Foreign Patents). See 37 CFR 1.51(d). Thus, some of the NPL documents were not considered since the references were not filed with the IDS.

Response to Arguments

Applicants contend that Olkin et al. fail to teach "wherein an entity comprises a user ID/client pair." Examiner respectfully disagrees. Olkin et al. teach a user ID and password which identify the users of the system (par. 79). The "/" appears between "user ID" and "client pair" indicating that one or the other is necessary to meet the limitation of the claim. Furthermore, even if the intended limitation is to have a user ID and client pair, Olkin et al. teach that the user ID and password are used with an email client (par. 75 and par. 79). Therefore, Olkin et al. teach wherein an entity comprises a user ID/client pair.

Furthermore, Applicants contend that "there is no teaching whatsoever in the cited paragraph of issuing a trust token for each entity successfully authenticating to said network service" and further "said trust token comprising a data object that includes a client identifier." Examiner respectfully disagrees. Olkin et al. teach that once the user using the client, i.e. process that allows for initiating secure transmission of email in the system, is authenticated as being eligible to send electronic messages securely, the server sends back a trust token including a key and message id for the message the client wishes to send (par. 46, par. 49, and par. 79). Before continuing with the response to Applicants submission, Examiner would first like to point out that in claim 3 Applicants have stated that a client may comprise of "an instance of a client software application." Since creation of a message is an instance of the client application (where the client application is software module which allows for email communications), the server's message including the message identifier and key transmitted back to the user are indeed types of client identifiers included within a data object of the trust token (par. 55-56). Thus, Olkin et al. teach wherein establishment of trusted entities occurs by issuing a trust token for each entity successfully authenticating to said network service, said trust token comprising a data object that includes a client identifier.

Applicants also contend that Olkin et al. fail to teach "said data object including: said user ID or a derivation thereof." Examiner respectfully disagrees. Olkin et al. teach that the data object includes the recipient's id, i.e. the user's ID in par. 51. Thus, Olkin et al. teach said data object including: said user ID or a derivation thereof.

Applicants further contend that Olkin et al. fail to teach "encrypting said trust token." Examiner respectfully disagrees. Olkin et al. teach sending the trust token, which comprises all

the elements disclosed as being contained within the data object, back in an encrypted format via an SSL channel (par. 115-117). Thus, Olkin et al. teach encrypting said trust token.

Applicants also contend that Olkin et al. fail to teach "transmitting said trust token from said network service to said client upon successful authentication to said network service by said entity." Examiner respectfully disagrees. Olkin et al. teach that a user/client must be authenticated as being allowed to send secure email, where once this authentication process is successful, the trust token with the message ID and message key, along with other elements, may be transmitted to the client in par. 114-115. Thus, Olkin et al. teach transmitting said trust token from said network service to said client upon successful authentication to said network service by said entity.

Applicants further contend that Olkin et al. fail to teach "storing said issued trust token." Examiner respectfully disagrees. Olkin et al. teach the use of a database to store tables containing trust tokens that have been issued for email that has been secured in par. 73-76. Thus, Olkin et al. teach storing said issued trust token.

Applicants also contend that Olkin et al. fail to teach "transmitting said stored issued trust token along with said user ID, authentication credentials, and client identifier from said client to said network service." Examiner respectfully disagrees. Olkin et al. not only teach saving the user ID (par. 95), but also that a database stores other elements such as a message ID, message key, and the user's password which is used as an authentication credential (par. 74-77). Thus, Olkin et al. teach transmitting said stored issued trust token along with said user ID, authentication credentials, and client identifier from said client to said network service.

Applicants further contend that Olkin et al. fail to teach "transmitting said stored, issued trust token occurs via a secure channel." Examiner respectfully disagrees. Olkin et al. teach sending the trust token, which comprises all the elements disclosed as being contained within the data object including the message ID and message key which are client identifiers, back in an encrypted format via an SSL channel, i.e. secure channel (par. 115-117). Thus, Olkin et al. teach transmitting said stored, issued trust token occurs via a secure channel.

Applicant also contends that Olkin et al. fail to teach "storing said issued trust token in a server side database, indexed according to a combination of a user ID and client identifier." Examiner respectfully disagrees. Olkin et al. teach that the database which maintains the trust token is on the server side and that the user ID, the email address, the message ID, and message key allow one to obtain various other fields in relation to the trust token (par. 73-77). Thus, Olkin et al. teach storing said issued trust token in a server side database, indexed according to a combination of a user ID and client identifier.

Applicant further contends that Olkin et al. fail to teach "transmitting said client identifier assigned by said network service from said network service to said client upon successful authentication to said network service by said entity." Examiner respectfully disagrees. Olkin et al. teach that the user must first be authenticated as being allowed to send secure emails and once that authentication is successful, a message ID and message key unique to that client instance of the software application are sent back to the client (par. 114-115). Thus, Olkin et al. teach transmitting said client identifier assigned by said network service from said network service to said client upon successful authentication to said network service by said entity.

Applicants also contend that Olkin et al. fail to teach "transmitting said user ID and client identifier to said server; and retrieving said stored trust token from said database." Examiner respectfully disagrees. Olkin et al. teach that once the authentication is successful the message key and message ID may be retrieved by the client in order to compose a secure email (par. 114-117). Thus, Olkin et al. teach transmitting said user ID and client identifier to said server; and retrieving said stored trust token from said database.

Applicants further contend that Olkin et al. fail to teach "wherein said server side database serves a plurality of services." Examiner respectfully disagrees. Olkin et al. teach that the database server provides for sending and receiving secured mail, i.e. a plurality of services (par. 43). Thus, Olkin et al. teach wherein said server side database serves a plurality of services.

Applicants also contend that Olkin et al. fail to teach "validating said trust token; and processing request without adding incremented response latency." Examiner respectfully disagrees. Olkin et al. teach a process of validating the trust token when the recipient of the secure email attempts to read the email (par. 133-141). Thus, Olkin et al. teach validating said trust token; and processing request without adding incremented response latency

Applicants further contend that Olkin et al. fail to teach "verifying that the user ID and a client identifier in the trust token match those presented by the client on the request." Examiner respectfully disagrees. Olkin et al. teach the user ID and the message ID in the trust token must match the stored trust token information in order to display the email (par. 141-143). Thus, Olkin et al. teach verifying that the user ID and a client identifier in the trust token match those presented by the client on the request.

Applicants also contend that Olkin et al. fail to teach "adding a configurable amount of incremental response latency when processing untrusted logins." Examiner respectfully disagrees. Olkin et al. teach that a recipient not authorized to receive secure email, i.e. an untrusted login, must first register with the system, where this step results in adding a specified amount of incremental response latency (par. 131 and par. 140-141). Thus, Olkin et al. teach adding a configurable amount of incremental response latency when processing untrusted logins.

Applicants further contend that Olkin et al. fail to teach "wherein untrusted logins include successful and unsuccessful logins from entities not bearing a trust token." Examiner respectfully disagrees. Olkin et al. teach that registered and unregistered users try to compose of gain access to the secure mail messages and that if a password entered is incorrect it eventually leads to an "unsuccessful" login and that if a user ID and password are entered correctly then it is a "successful" login (par. 112-114). Thus, Olkin et al. teach wherein untrusted logins include successful and unsuccessful logins from entities not bearing a trust token.

Applicants also contend that Olkin et al. fail to teach "wherein said policies are applied by a server" and also that it has not been established that "there are different policies for handling trusted logins and untrusted logins." Examiner respectfully disagrees. Olkin et al. teach a server which allows registered users to compose and receive secure email, i.e. a policy for handling trusted logins (par. 43). Olkin et al. further teach that if the user is not registered, he/she is considered untrusted and therefore will not pass the authentication process which would allow viewing the email until the user has registered (if he/she chooses to), i.e. a different policy for untrusted logins (par. 141-142). Thus, Olkin et al. teach wherein said policies are applied by

a server, as well as that there are different policies for handling trusted logins and untrusted logins.

Applicants further contend that Olkin et al. and Morkel fail to teach/suggest "placing a hash of the user ID in a trust token." Examiner respectfully disagrees. Morkel suggests that in order to maintain a secure id (such as a user's email address), it is hashed before being stored (par. 7). Morkel provides motivation for modifying the method disclosed in Olkin et al. to hash the user ID provided in the trust token of Olkin et al. because Morkel suggests that using a hash of the user's id secures the id from being compromised in par. 7. Thus, the combination of Olkin et al. and Morkel teach/suggest placing a hash of the user ID in a trust token.

Applicants also contend that Olkin et al. and Pallante fail to teach/suggest "the combination of including time stamps in a trust token." Examiner respectfully disagrees. Olkin et al. teach the use of a trust token and even further storing that trust token (par. 73-76). Pallante suggests maintaining logs with timestamps of when users were authenticated in order to access documents (par. 154). Pallante provides motivation for modifying the trust token disclosed in Olkin et al. to maintain a time stamp for each trust token used in an authentication step Pallante suggests that time-stamping and maintaining a log with the time-stamping information is important in non-repudiation proofs in par 154. Furthermore, in response to Applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Thus, the combination of Olkin et al. and Pallante teach/suggest the combination of including time stamps in a trust token.

Applicants further contend that Olkin et al. and Pallante fail to teach "that a trust token may be a certificate." Examiner respectfully disagrees. Applicants made this argument with respect to claims 37 and 74, where no mention is made of a certificate being the trust token. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., wherein the trust token may be a certificate) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Applicants also contend that Olkin et al. fail to teach "the record created includes the originating network address." Examiner respectfully disagrees. Since the term network address is broad, an email address is also considered to be a type of net address so the Examiner maintains that Olkin et al. teach that the since the record contains the sender's email address, Olkin et al. teach the record containing an originating network address in par. 79.

Applicants further contend that Olkin et al. fail to teach "that an existing record is updated with each successful authentication." Examiner respectfully disagrees. Olkin et al. teach that a sent-mail table is stored with reference to a record (par. 47 and par. 60-61) and that the sender may define a number of times that the email may be read/accessed which is updated to ensure the maximum number of reads is not mistakenly/maliciously exceeded (par. 66). Thus, Olkin et al. teach that an existing record is updated with each successful authentication.

Applicants also contend that Olkin et al. fail to teach "that the user is requesting network service from an anonymous client." Examiner respectfully disagrees. Olkin et al. teach that when the secure server sends the recipient the email, that recipient may not be registered with that

particular service and thus is anonymous to the secure email service (par. 46). Thus, Olkin et al. teach that the user is requesting network service from an anonymous client.

Applicants further contend that Olkin et al. and Roux et al. fail to teach/suggest "a valid time period" or "configurable percentage of successful trusted logins." Examiner respectfully disagrees. Roux et al. teach that if a response is not received within a valid time period, the user is deemed untrustworthy (par. 47). Roux et al. suggest motivation to modify the method disclosed in Olkin et al. to add a response latency to untrusted logins to determine whether or not certain user profiles should not be trusted because Roux et al. suggest that a response should be received within a valid period of time in order to further determine whether or not a certain user is trustworthy in par. 47. Thus, the combination of Olkin et al. and Roux et al. teach/suggest a valid time period and configurable percentage of successful trusted logins.

Applicants also contend Olkin et al. and Card fail to teach/suggest "wherein processing remaining requests according to at least a second policy comprises requiring and untrusted entity to comprise a Turing test." Examiner respectfully disagrees. Card teaches that the server automatically may question the user based on information that only the user would know allows for stronger authentication and determining if the response is a human/user-generated response or not (par. 43). Card provides motivation to modify the method disclosed in Olkin et al. to subject an untrusted entity to complete a Turing test in order to determine whether or not that user is a valid user or if the user should remain untrusted since Card suggests that requiring the user to answer a security question, which is known only to that user, in order to establish whether or not he/she should be trusted allows for stronger authentication in par. 43. Thus, the combination of Olkin et al. and Card teach/suggest wherein processing remaining requests

according to at least a second policy comprises requiring and untrusted entity to comprise a Turing test.

Applicants further contend that Olkin et al. and Roux et al. fail to teach/suggest "wherein a network address comprises an IP (internet protocol) address" and further that "even if Roux were to contain such teaching, Roux offers no support for the Examiner's position." Examiner respectfully disagrees. First, Examiner would like to point out that the previous network address defined in claim 75 was "an originating network address" where claim 77 makes reference to "a network address" which as claimed does not refer to the previously defined "originating network address" and thus these two network addressed are different where Roux et al. suggests the use of a network address comprising an IP address. Roux et al. teach that if the IP address is authenticated, it adds a stronger means of authentication when used in combination with other factors (par. 47). Roux et al. provide motivation to modify the method disclosed in Olkin et al. for a network address include an IP address since Roux et al. suggest that using an IP address adds a stronger means of authentication when used in combination with other user information in par. 47.

Due to the reasons stated above, the Examiner maintains rejections with respect to pending claims. The cited prior arts teach the limitations that the Applicant suggests distinguish from the prior art. Therefore, it is the Examiner's conclusion that the pending claims are not patentably distinct or non-obvious over the prior art of record as presented.

Claim Objections

Claims 3-4 and 33-34 are objected to because of the following informalities: These claims depend on claim 2, which was cancelled in the amendment to the claims filed 11/17/2006. Appropriate correction is required.

Claims 40 and 72 are objected to because of the following informalities: These claims depend on claim 39 which was cancelled in the amendment to the claims filed 11/17/2006. Appropriate correction is required.

Claim Rejections - 35 USC § 102

III. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

IV. Claims 1, 3-5, 8, 38, 40-42, 45, 12-28, 30-31, 35, 49-65, 67-68, and 72 are rejected under 35 U.S.C. 102(e) as being fully anticipated by Olkin et al., US Pub. No., 2003/0046533.

As per claims 1 and 38:

Olkin et al. teach a method/computer program product on a computer readable medium, comprising the steps of: identifying entities legitimately entitled to service, wherein an entity comprises a user ID/client pair (par. 45); establishing said identified entities as trusted entities by issuing a trust token for each entity successfully authenticating to said network service, said trust token comprising a data object that includes a client identifier (par. 45); processing requests from

said trusted entities according to a first policy (par. 45 and par. 46, lines 1-4); and processing remaining requests according to at least a second policy (par. 46, lines 4-9).

As per claims 3 and 40:

Olkin et al. teach the method/computer program product on a computer readable medium of claims 2 and 39. Furthermore, Olkin et al. teach wherein said client comprises any of: an instance of a client software application; and a machine running a client software application (par. 46).

As per claims 4 and 41:

Olkin et al. teach the method/computer program product on a computer readable medium of claims 2 and 40. Furthermore, Olkin et al. teach wherein entities legitimately entitled to service comprise entities previously able to successfully authenticate to a network service (par. 46).

As per claims 5 and 42:

Olkin et al. teach the method/computer program product on a computer readable medium of claims 4 and 41. Furthermore, Olkin et al. teach wherein said network service comprises a server (par. 110).

As per claims 8 and 45:

Olkin et al. teach the method/computer program product on a computer readable medium of claims 1 and 38. Furthermore, Olkin et al. teach said data object including: said user ID or a derivative thereof (par. 49).

As per claims 12 and 49:

Olkin et al. teach the method/computer program product on a computer readable medium of claims 11 and 38. Furthermore, Olkin et al. teach said client identifier comprising any of: a client identifier assigned by said network service; and a client identifier provided by the client (par. 75).

As per claims 13 and 50:

Olkin et al. teach the method/computer program product on a computer readable medium of claims 7 and 45. Furthermore, Olkin et al. teach further comprising a step of encrypting said trust token (par. 74).

As per claims 14 and 51:

Olkin et al. teach the method/computer program product on a computer readable medium of claim 13 and 50. Furthermore, Olkin et al. teach further comprising the step of: transmitting said trust token from said network service to said client upon successful authentication to said network service by said entity (par. 115).

As per claims 15 and 52:

Olkin et al. teach the method/computer program product on a computer readable medium of claims 14 and 51. Furthermore, Olkin et al. teach wherein said step of transmitting said trust token occurs via a secure channel (par. 116).

As per claims 16 and 53:

Olkin et al. teach the method/computer program product on a computer readable medium of claims 15 and 52. Furthermore, Olkin et al. teach wherein said secure channel comprises a network connection secured via the SSL (secure sockets layer) protocol (par. 116).

As per claims 17 and 54:

Olkin et al. teach the method/computer program product on a computer readable medium of claims 7 and 49. Furthermore, Olkin et al. teach further comprising the step of: storing said issued trust token on said client (par. 95).

As per claims 18 and 55:

Olkin et al. teach the method/computer program product on a computer readable medium of claims 17 and 54. Furthermore, Olkin et al. teach further comprising the step of: transmitting said stored issued trust token along with said user ID, authentication credentials, and client identifier from said client to said network service (par. 76).

As per claims 19 and 56:

Olkin et al. teach the method/computer program product on a computer readable medium of claims 18 and 55. Furthermore, Olkin et al. teach wherein said step of transmitting said stored, issued trust token occurs via a secured channel (par. 85).

As per claims 20 and 57:

Olkin et al. teach the method/computer program product on a computer readable medium of claims 19 and 56. Furthermore, Olkin et al. teach wherein said secured channel comprises a network connection secured via the SSL (secure sockets layer) protocol (par. 85-86).

As per claims 21 and 58:

Olkin et al. teach the method/computer program product on a computer readable medium of claims 12 and 50. Furthermore, Olkin et al. teach further comprising a step of storing said issued trust token in a server side database, indexed according to a combination of user ID and client identifier (par. 74-75).

As per claims 22 and 59:

Olkin et al. teach the method/computer program product on a computer readable medium of claims 21 and 58. Furthermore, Olkin et al. teach further comprising the step of: transmitting said client identifier assigned by said network service from said network service to said client upon successful authentication to said network service by said entity (par. 103-109).

As per claims 23 and 60:

Olkin et al. teach the method/computer program product on a computer readable medium of claims 22 and 59. Furthermore, Olkin et al. teach wherein said step of transmitting said client identifier assigned by said network service occurs via a secure channel (par. 103).

As per claims 24 and 61:

Olkin et al. teach the method/computer program product on a computer readable medium of claims 22 and 59. Furthermore, Olkin et al. teach said secure channel comprising a network connection secured via the SSL (secure sockets layer) protocol (par. 103).

As per claims 25 and 62:

Olkin et al. teach the method/computer program product on a computer readable medium of claims 21 and 58. Furthermore, Olkin et al. teach further comprising the steps of: transmitting said user ID and client identifier to said server; and retrieving said stored trust token from said database (par. 114).

As per claims 26 and 63:

Olkin et al. teach the method/computer program product on a computer readable medium of claims 21 and 58. Furthermore, Olkin et al. teach wherein said server side database serves a plurality of services (par. 43).

As per claims 27 and 64:

Olkin et al. teach the method/computer program product on a computer readable medium of claims 2 and 40. Furthermore, Olkin et al. teach wherein processing requests from said trusted entities according to a first policy comprises the steps of: validating said trust token (par. 112); and processing request without adding incremental response latency (par. 114).

As per claims 28 and 65:

Olkin et al. teach the method/computer program product on a computer readable medium of claims 27 and 64. Furthermore, Olkin et al. teach wherein said step of validating said trust token comprises the step of: verifying that the user ID and a client identifier in the trust token match those presented by the client on the request (par. 112).

As per claims 30 and 67:

Olkin et al. teach the method/computer program product on a computer readable medium of claims 2 and 40. Furthermore, Olkin et al. teach wherein processing remaining requests according to at least a second policy comprises adding a specified amount of incremental response latency when processing untrusted logins (par. 140).

As per claims 31 and 68:

Olkin et al. teach the method/computer program product on a computer readable medium of claims 30 and 67. Furthermore, Olkin et al. teach wherein untrusted logins include successful and unsuccessful logins from entities not bearing a trust token (par. 112).

As per claims 35 and 72:

Olkin et al. teach the method/computer program product on a computer readable medium of claims 1 and 39. Furthermore, Olkin et al. teach wherein said policies are applied by a server (par. 115).

Claim Rejections - 35 USC § 103

VI. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

VII. Claims 9 and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Olkin et al., US Pub. No., 2003/0046533 as applied to claims 8 and 45 above, and further in view of Morkel, US Patent No. 2002/0052921.

As per claims 9 and 46:

Olkin et al. substantially teach the method/computer program product on a computer readable medium of claims 8 and 45. Not explicitly disclosed is wherein said derivative comprises a cryptographic hash of the user ID. However, Morkel teaches that in order to maintain a secure id, it is hashed before being stored. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Olkin to hash the user ID in order to maintain security. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Morkel suggests that using a hash of the user's id secures the id from being compromised in par. 7.

VIII. Claims 10, 29, 37, 47, 66, 74-76, 78-87, and 93 are rejected under 35 U.S.C. 103(a) as being unpatentable over Olkin et al., US Pub. No., 2003/0046533 as applied to claims 6, 8, 28, 44-45, and 65 above, and further in view of Pallante, US Pub. No. 2003/0028495.

As per claims 10 and 47:

Olkin et al. substantially teach the method/computer program product on a computer readable medium of claims 8 and 45. Not explicitly disclosed is wherein said data object further includes any of: a time stamp of first authentication to said network service by said entity; and a time stamp of a most recent authentication to said network service by said entity. However, Pallante teaches that logs are kept with timestamps of when users were authenticated in order to access documents. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Olkin et al. to maintain a time stamp for a first and most recent authentication when the entity accesses the system. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Pallante suggests that time-stamping and maintaining a log with the time-stamping information is important in non-repudiation proofs in par 154.

As per claims 29 and 66:

Olkin et al. substantially teach the method/computer program product on a computer readable medium of claims 28 and 65. Not explicitly disclosed is wherein said step of validating said trust token further comprises any of the steps of: verifying that a time stamp of a first authentication by the entity recorded in the trust token is no earlier than a configurable earliest acceptable first-authentication time stamp; and verifying that a time stamp of a last authentication by the entity recorded in the trust token is no earlier than a configurable earliest acceptable last-authentication time stamp. However, Pallante teaches wherein the token is a certificate which holds a validity period of when the entity can gain access to the system. Therefore, it would have been obvious to a person in the art at the time the invention was made

to modify the method disclosed in Olkin et al. to enhance the security of the system by using a certificate instead of a password as the trust token and to allow access based on the validity period as defined by the certificate. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Pallante suggests that using a certificate and abiding by the validity periods in important to ensure that entities do not gain access unless they are allowed based on their privileges in par. 99.

As per claims 37 and 74:

Olkin et al. substantially teach the method/computer program product on a computer readable medium of claims 6 and 38. Not explicitly disclosed is further comprising the step of: updating said trust token after a login by a trusted entity. However, Pallante teaches that the trusted token may be a certificate in order to increase security, as well as renewing certificates when appropriate. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Olkin et al. to use a certificate as the trust token and to renew it when necessary. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Pallante suggests that renewing a certificate will further ensure that appropriate entities gain access to resources for the full duration of the amount of time they are entitled to do so in par. 51.

As per claim 75:

Olkin et al. teach a method of establishing an entity requesting a network service as trusted, comprising the steps of: for each successful authentication, adding or updating a

database record containing at least a user identifier, an originating network address (par. 79); comparing all subsequent authentication requests to said record; and where the user identifier of a subsequent request matches that of a successful authentication, extending trust to the subsequent request if its originating network address satisfy predetermined criteria in relation to said record (par. 45 and 51).

Not explicitly disclosed are a date/timestamp of first and/or the current successful authentication and wherein the timestamp information satisfies predetermined criteria in relation to said record. However, Pallante teaches that a timestamp is used in order to increase the system's integrity and indicate normalcy when the timestamps fall within some predetermined criteria. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Olkin et al. to maintain a time stamp for a first and most recent authentication when the entity accesses the system and to test the timestamp information against previous time-stamping information in regards to the stored record. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Pallante suggests that time-stamping and maintaining a log with the time-stamping information where the current time is compared with the stored record is important in non-repudiation proofs and in maintaining the integrity of the user database in par. 61.

As per claim 76:

Olkin et al. and Pallante substantially teach the method of claim 75. Furthermore, Olkin et al. teach wherein said step of adding or updating a database record comprises either of the steps of: creating a new record by said network service if an entity has not previously

authenticated to said network service (par. 46); and updating a previously created record for subsequent authentication requests from said entity (par. 47).

As per claim 78:

Olkin et al. and Pallante substantially teach the method of claim 75. Furthermore, Pallante teaches wherein the step of extending trust to the subsequent request comprises: extending trust if the user identification and originating network address match those of the record exactly, and wherein the data/timestamps from the record satisfy specified bounds checks (par.156).

As per claim 79:

Olkin et al. and Pallante substantially teach the method of claim 75. Furthermore, Pallante teaches wherein the step of extending trust to the subsequent request comprises: when the user identifier of the subsequent request matches that of a record, determining a trusted address range, defined by client addresses from which successful authentications have originated, for the user identifier from stored authentication records (par. 79).

As per claim 80:

Olkin et al. and Pallante substantially teach the method of claim 79. Furthermore, Olkin et al. teach wherein the step of extending trust to the subsequent request further comprises: determining if the originating address of the subsequent request falls within the trusted address range (par. 79), and Pallante teaches determining if the data/timestamps for the trusted address range satisfy specified bounds checks (par. 156).

As per claim 81:

Olkin et al. and Pallante substantially teach the method of claim 79. Furthermore, Pallante teaches wherein the step of determining if the data/timestamps for the trusted address range satisfy configurable bounds checks comprises the steps of: establishing earliest date/timestamp for the trusted address range as a minimum for the earliest authentication timestamp; and establishing earliest date/timestamp for the trusted address range as a maximum for the earliest authentication timestamp (par 156).

As per claim 82:

Olkin et al. and Pallante substantially teach the method of claim 79. Furthermore, Pallante teaches wherein the step of extending trust to the subsequent request further comprises: if the timestamps pass specified bounds checks, extending trust to the request (par. 156).

As per claim 83:

Olkin et al. and Pallante substantially teach the method of claim 75. Furthermore, Olkin et al. teach wherein the entity comprises a user requesting the network service from an anonymous client (par. 46).

As per claim 84:

Olkin et al. and Pallante substantially teach the method of claim 83. Furthermore, Olkin et al. teach wherein the network service comprises a server (par. 110).

As per claim 85:

Olkin et al. and Pallante substantially teach the method of claim 84. Furthermore, Olkin et al. teach wherein the client and the server are in communication via a secured network channel (par. 103).

As per claim 86:

Olkin et al. and Pallante substantially teach the method of claim 85. Furthermore, Olkin et al. teach said secure channel comprising a network connection secured via the SSL (secure sockets layer) protocol (par. 103).

As per claim 87:

Olkin et al. and Pallante substantially teach the method of claim 75. Furthermore, Olkin et al. teach further comprising the steps of: processing requests from trusted entities according to a first policy (par. 46, lines 1-4; and processing remaining requests according to at least a second policy (par. 46, lines 4-6).

As per claim 93:

Olkin et al. and Pallante substantially teach the method of claim 87. Furthermore, Olkin et al. teach wherein said policies are applied by a server (par. 110).

IX. Claims 32-33, 36, 69-70, and 73 are rejected under 35 U.S.C. 103(a) as being unpatentable over Olkin et al., US Pub. No., 2003/0046533 as applied to claims 8 and 45 above, and further in view of Roux et al., US Pub. No. 2002/0042883.

As per claim 32:

Olkin et al. substantially teach the method of claim 31. Not explicitly disclosed is wherein response latency is added to a configurable percentage of successful untrusted logins. However, Roux et al. teach that if a response is not received within a valid time period, the user is deemed untrustworthy. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Olkin et al. to add a response latency to untrusted logins to determine whether or not certain user profiles should not be trusted. This modification would have been obvious because a person having ordinary skill in the art, at the

time the invention was made, would have been motivated to do so since Roux et al. suggest that a response should be received within a valid period of time in order to further determine whether or not a certain user is trustworthy in par. 47.

As per claims 33 and 70:

Olkin et al. substantially teach the method/computer program product on a computer readable medium of claims 2 and 40. Not explicitly disclosed is wherein processing remaining requests according to at least a second policy comprises adding a specified amount of incremental response latency when processing requests from untrusted IP addresses that have exceeded a configurable login rate. However, Roux et al. teach that if a response is not received within a valid time period, the user is deemed untrustworthy. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Olkin et al. to add a response latency to untrusted logins to determine whether or not certain user profiles should not be trusted. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Roux et al. suggest that a response should be received within a valid period of time in order to further determine whether or not a certain user is trustworthy in par. 47.

As per claims 36 and 73:

Olkin et al. substantially teach the method/computer program product on a computer readable medium of claims 35 and 39. Not explicitly disclosed is wherein said server applies rate policies for a plurality of network devices. However, Roux et al. teach that if a response is not received within a predetermined time period, the user is deemed untrustworthy and the communication is discarded. Therefore, it would have been obvious to a person in the art at the

time the invention was made to modify the method disclosed in Olkin et al. for the server to apply a rate policy for the network devices. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Roux et al. suggest that a response should be received within a valid period of time in order to further determine whether or not a certain user is trustworthy in par. 37.

As per claim 69:

Olkin et al. substantially teach the computer program product on a computer readable medium of claim 68. Not explicitly disclosed is wherein response latency is added to a specified percentage of successful logins. However, Roux et al. teach that if a response is not received within a valid time period, the user is deemed untrustworthy. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Olkin et al. to add a response latency to untrusted logins to determine whether or not certain user profiles should not be trusted. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Roux et al. suggest that a response should be received within a valid period of time in order to further determine whether or not a certain user is trustworthy in par. 47.

X. Claims 34 and 71 are rejected under 35 U.S.C. 103(a) as being unpatentable over Olkin et al., US Pub. No., 2003/0046533 as applied to claims 2 and 40 above, and further in view of Card, US Pub. No. 2002/0073339.

As per claims 34 and 71:

Olkin et al. substantially teach the method/computer program product on a computer readable medium of claims 2 and 40. Not explicitly disclosed is wherein processing remaining requests according to at least a second policy comprises requiring an untrusted entity to complete a Turing test. However, Card teaches that questioning the user based on information that only the user would know allows for stronger authentication. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Olkin et al. (as modified with Pallante) to subject an untrusted entity to complete a Turing test in order to determine whether or not that user is a valid user or if the user should remain untrusted. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Card suggests that requiring the user to answer a security question, which is known only to that user, in order to establish whether or not he/she should be trusted allows for stronger authentication in par. 43.

XI. Claims 77, 88-91 and 94 are rejected under 35 U.S.C. 103(a) as being unpatentable over Olkin et al., US Pub. No., 2003/0046533 and Pallante, US Pub. No. 2003/0028495 as applied to claims 75 and 87 above, and further in view of Roux et al., US Pub. No. 2002/0042883.

As per claim 77:

Olkin et al. and Pallante substantially teach the method of claim 75. Not explicitly disclosed is wherein a network address comprises an IP (internet protocol) address. However, Roux et al. teach that if the IP address is authenticated, it adds a stronger means of authentication when used in combination with other factors. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Olkin et al. (as modified with Pallante) for the network address to also include an IP address. This modification

would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Roux et al. suggest that using an IP address adds a stronger means of authentication when used in combination with other user information in par. 47.

As per claim 88:

Olkin et al. and Pallante substantially teach the method of claim 87. Not explicitly disclosed is wherein processing remaining requests according to at least a second policy comprises adding a configurable amount of incremental response latency when processing untrusted logins. However, Roux et al. teach that if a response is not received within a valid time period, the user is deemed untrustworthy. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Olkin et al. (as modified with Pallante) to add a response latency to untrusted logins to determine whether or not certain user profiles should not be trusted. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Roux et al. suggest that a response should be received within a valid period of time in order to further determine whether or not a certain user is trustworthy in par. 47.

As per claim 89:

Olkin et al., Pallante, and Roux et al. substantially teach the method of claim 88. Furthermore, Roux et al. teach wherein untrusted logins include successful and unsuccessful logins from untrusted entities (par. 47).

As per claim 90:

Olkin et al., Pallante, and Roux et al. substantially teach the method of claim 89. Furthermore, Roux et al. teach wherein response latency is added to a configurable percentage of successful untrusted logins (par.47).

As per claim 91:

Olkin et al. and Pallante substantially teach the method of claim 87. Not explicitly disclosed is wherein processing remaining requests according to at least a second policy comprises adding a configurable amount of incremental response latency when processing requests from IP addresses that have exceeded a configurable login rate. However, Roux et al. teach that if a response is not received within a valid time period, the user is deemed untrustworthy. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Olkin et al. (as modified with Pallante) to add a response latency to untrusted logins to determine whether or not certain user profiles should not be trusted. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Roux et al. suggest that a response should be received within a valid period of time in order to further determine whether or not a certain user is trustworthy in par. 47.

As per claim 94:

Olkin et al., Pallante, and Roux et al. substantially teach the method of claim 91. Not explicitly disclosed is wherein said server applies rate policies for a plurality of network devices. However, Roux et al. teach that if a response is not received within a predetermined time period, the user is deemed untrustworthy and the communication is discarded. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method

disclosed in Olkin et al. (as modified with Pallante and Roux et al.) for the server to apply a rate policy for the network devices. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Roux et al. suggest that a response should be received within a valid period of time in order to further determine whether or not a certain user is trustworthy in par. 37.

XII. Claim 92 is rejected under 35 U.S.C. 103(a) as being unpatentable over Olkin et al., US Pub. No., 2003/0046533 and Pallante, US Pub. No. 2003/0028495 as applied to claim 87 above, and further in view of Card, US Pub. No. 2002/0073339.

As per claim 92:

Olkin et al. and Pallante substantially teach the method of claim 87, wherein processing remaining requests according to at least a second policy comprises requiring an untrusted entity to complete a Turing test. However, Card teaches that questioning the user based on information that only the user would know allows for stronger authentication. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Olkin et al. (as modified with Pallante) to subject an untrusted entity to complete a Turing test in order to determine whether or not that user is a valid user or if the user should remain untrusted. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Card suggests that requiring the user to answer a security question, which is known only to that user, in order to establish whether or not he/she should be trusted allows for stronger authentication in par. 43.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Nadia Khoshnoodi
Examiner
Art Unit 2137
5/26/2007

NK

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER